RESPONSE TO OFFICE ACTION

Applicant responds to the Office Action as set forth herein.

Kindly amend the claims as set forth on the following pages.

Applicant submits remarks as follows.

REMARKS

Applicant notes with gratitude that the previous grounds of rejection are considered moot. Claims 1, 2 and 6 now stand rejected as being supposedly anticipated in view of US-A-6,990,591 (Pearson), not previously cited. The Examiner puts forth the view that Pearson supposedly discloses all features of claims 1, 2 and 6 and that these claims therefore lack novelty in view of Pearson. As will be explained below, is respectfully submitted that these claims are novel over Pearson and the amendments made herewith to claims 1 and 6, for example, further clarify the distinction of the present invention over the disclosure of Pearson.

Pearson relates to computer network security and to methods and systems for remotely monitoring the security status of a computer network. Importantly, as explained at column 8, lines 10 to 57, the intrusion detection system functions based on the use of "attack signatures". An unfiltered communication is inspected for the presence of "predetermined attack signatures" by comparing it to a list of known attack signatures. Figure 9 shows an example of some "attack signatures". As can be seen, the attack signatures include both a header 810 which includes both an IP address 812 and a port number 814. The IP address is the destination address of the communication device. In addition, the attack signature includes a body 820 including a message field 822 and a content field 824. As indicated at column 19, lines 24 to 26, the content field 834 comprises the actual character string entered by the source of the communication. An example is given of how a string "user route lodl" represents the exact sequence of characters that would be entered by a person (such as a hacker) attempting to enter an ftp-capable server and issue commands at the "root level" of access. In other words, the attack signatures include the syntax of messages that are thought of as potentially worthy of attention by the intrusion detection system.